DIGITAL FORENSIC ANALYSIS FOR IMPROVING INFORMATION SECURITY

Asra Ahmadi[1]

[1]*M.Tech Student, PDA Engineering College, Kalaburagi, Karnataka, India*

---***---

Abstract -*Digital evidence plays a very important role because it is used to connect individuals to illegal activities. Ensuring the credibility, reliability, and audit of digital evidence is of severe significance.A system is proposed which allows the authorize person to monitor the behaviour of users and make a analysis based on user activity, and recognize any attacker or malicious behaviour and securing the identity of such malicious users for the Chain of Custody process which is then introduced to court of law.*

Key Words: **Digital forensics, forensic analysis, information security**

1. INTRODUCTION

When it comes to digital evidence, digital forensics is a field of Forensic-Science which focuses on meticulous extraction and extraction of digital evidence with goal of making it acceptable in court without raising any concerns about evidence's integrity.CoC is nothing more than the consecutive documents documenting the custody, control, transition, examination, and physical or electronic evidence order. During the investigation and the process of presenting the facts in court, CoC requires risky measures. Each and every person is liable for the proof he / she takes. Any indication of a shift in facts will, at the time raised in court[1], prove invaluable. The goal of cyber security is to keep networks and devices safe from outside attacks. Confidentiality, authenticity, as well as accessibility, or CIA, is industry standard for Cyber Security. Systems, functions and information must be accessible on with agreed-upon norms for integrity and confidentiality, as well as for access. Availability also implies that only authorised parties may access data. Authentication procedures are most important part of Cyber Security. Passwords are used to verify that consumer is who they say they are and that they have correct credentials to access an account. As a technology user, you need to know and comprehend digital forensics and cyber security in order to protect yourself and your data. Understanding both and also how they work together is critical to ensuring the security of your personal information. Cybercriminals often attempt to benefit from their crimes via a number of methods, including:

Denial of Service, or DOS,Malware ,Man in the Middle ,Phishing .Other types of cyberattacks include cross-site scripting attacks, password attacks, eavesdropping attacks (that could be physical), SQL-injection attacks, also birthday attacks based upon algorithm functions. The proposed system puts light on attackes like DDos (Distributed denial of service) and Brute-force attack.

2 Related Works

In this section we briefly overview related works of Digital forensic analysis and information security.

Haque M M, Hossain S proposes a system for the handling of the analysis's residual data, with a technique geared toward both reactive and proactive forensic investigations. To help investigators, this study developed forensically ready common standard digital forensics framework that is complete[2]. In order to facilitate a methodical postmortem of digital forensics, the suggested framework has been designed Though theoretical, the suggested framework will be assessed and put into practise with the help of an expert system into future.

Ezhil Kalaimannan presented a novel concept, giving a preparatory investigation on the administration of advanced prove and the innovations that can be utilized to actualize it with security ensures in IoT situations for the individual gadgets to characterize the concept of computerized witnesses, where individual gadgets are able to effectively obtain, store, and transmit advanced prove to an authorized substance dependably and safely[3].

Through antiforensics, the researchers want to improve data security[4]. Some basic anti-forensic approaches are examined, and a representative sampling of free and commercial memory acquisition technologies are tested. To determine whether existing forensic tools can withstand basic anti-forensic measures, they presented a nocel memory collection approach, and then evaluated suchmethod's additional susceptibility foragitating by examining much complex anti-forensic measures. Without operating system support, they employed direct page table manipulations using PCI hardware contemplation approach. Their work is limited by the fact that it relies upon this OS to locate page tables.

The authors Singh, S., & Singh, N has analyzed the huge amount of digital evidence should submit to court for the purpose punish the culprit and evidence should submitted in digitally way which means truthful, because of more number of evidence they developed a forensics software to collect the multiple data , locations for they found the Advanced forensics Format(AFF) in the new networks to built the quality of chain of custody[5].

Digital evidence preservation and identification, information analysis and extraction, as well as time-critical decision-making, are primary goals of digital forensic investigations. A new Digital Evidence Object (DEO) paradigm for reducing forensic data in digital forensic inquiry has been proposed and described here by researchers[6]. Depending upon this synergy of categories analysis as well as integrating 5Ws (Who, What, Where and When and Why) of digital investigative methodologies for digital evidence collecting, the DEO model was created. They use a real-world case study to show how it may aid computer forensics specialists in analysis of digital evidence. Their findings show that DEO model may significantly reduce amount of false positive evidence objects provided to forensics expert, thereby decreasing his/her workload and boosting decision-making performance in such time-critical environment.

Data Fusion for Countering Anti-Forensics." Data Fusion in Counter-Anti-Forensic (CAF) situation is being studied to see whether there is a benefit to using it. An evidence-based framework, known as D-Shafer Theory of Evidence, was used in their technique. Synergistically merging information supplied by IF and CAF tools, they wanted to uncover traces of anti-forensic algorithms, and they wanted accounting for non-trivial interactions among CAF and IF [7] [8].

3. Module Description

This section describes the modules of the proposed system. There are three modules in the proposed system Admin, User and Attacker module. Each module describes characteristics and activities of specific users

3.1. User

There are n number users present in this module. Before doing any actions, the user must first log in. A user's information will be saved in database when they register. After completing the registration process, he is required to log in using the user name and passcode that he was assigned. Once a user has successfully logged in, he or she may undertake a variety of tasks, including searching for other members, seeing friend requests, viewing all of his or her friends and deleting them, posting images and messages, and login history account status and more.

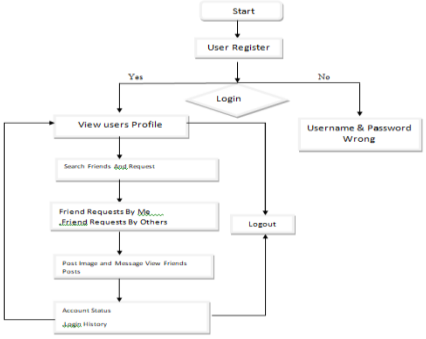
Start
User Register
Yes
No
Login
View users Profile
Username & Password Wrong
Search Friends And Request
Friend Requests By Me
Friend Requests By Others
Logout
Post Image and Message View Friends Posts
Account Status
Login History

Fig1: flowchart for user

3.1.1Algorithm for User

1: Select the type of user(admin /user)

2:if the user is admin ,go to step 3

3: the user has to login and if user is valid password then they view the profile then ,go to next step.

4: user can search friends and send them request and by others friends request to user.

5: user can check status and login history

6: if the invalid password then go back to step

7: click logout button.

3.2. Server

This module requires Server to authenticate itself with valid username and password. View Users and Authorizations, All Friends and Status, All Users Posts, and more may be done after a successful login. DDOS Attackers View a list of all Crimeware users. See Every Regular User Accounts, View All Spam User Behaviour, Behaviours shown by normal users are shown below. View Spam Users Chart, View DDOS Users Chart.

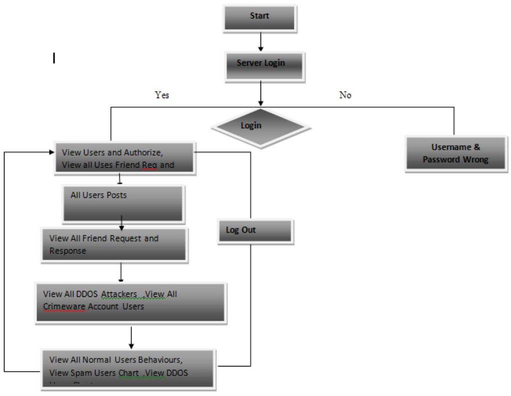
Start
Server Login
Yes
No
Login
View Users and Authorize, View all Uses Friend Req and
Username & Password Wrong
All Users Posts
Log Out
View All Friend Request and Response
View All DDOS Attackers ,View All Crimeware Account Users
View All Normal Users Behaviours, View Spam Users Chart ,View DDOS

Fig2: Flow chart for server

3.2.2 Algorithm for server

.Step 1:click start button

2Step 2: sever can login with valid password and can view the users authorised and request and response by user friends

Step3: server can view all the posts of user

Step 4: server can also block DDOS attackers and crimeware account of user

Step 5: At last the server can view spam chart users and also usersbehaviours or DDOS user chart.

Step 6:server can logout.

3.3. Attacker

In this module,we have demonstrate how attacker try to attempnumerous attacks likeDdos(distributed denial of service) and Brute-force attack.

3.3.1 DDoS

Distributed denial of service (DDoS) attacks are malicious attempts for disrupting normal traffic upon a server or service by flooding target and its associated functions by Internet traffic. These attacks aim to cause a denial of service by draining the target's resources. Most of time, goal of attackers is to impede proper operation of the online resources. In other cases, attacker may demand compensation for halting attack, or they may attempt to harm or defame competitor's company.

3.3.2 Brute Force Attack:

Passwords, login credentials, including encryption keys are all susceptible to brute force attacks, which are based upon principle of learning by doing. Unauthorized access to computer systems and networks, whether of personal or business nature, may be gained by this simple but effective method. The hacker tries a variety of usernames and passwords, frequently on computer, until they discover proper credentials.

4. ANALYSIS

Proposed system aids in digital forensics by allowing the server to secure the activities of users in database and make an analysis based on the history of the user and user activity. In this system analysis of compromised accounts is done by monitoring its users and their activity. If there is an attempt of DDos attack on other user then the admin can identify the victims account and number of times the attack has performed and led the user under attack to change his/her password and make their account secure. An analysis of spam accounts(fig:4) is done by monitoring the comments and posts of the users if they uses negative comments on posts or posts any improper files or sends too many friend requests to other users to make them disturb.If there is an attempt of bruteforce attack the victims account get blocked and admin can identify it by monitoring the status of users account.

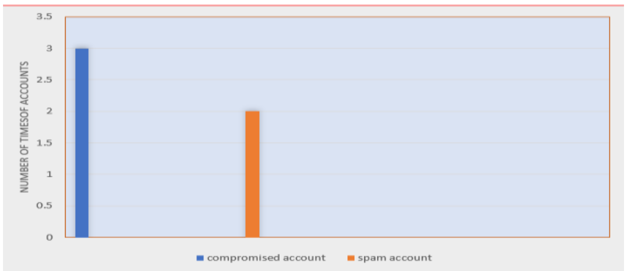

Fig:3 Comparision between Compromised account and Spam account

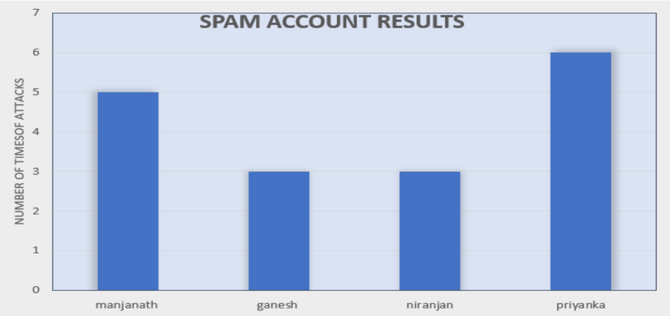

Fig:4 Spam account analysis

5. CONCLUSION

In the proposed system we have given authority to admin to monitor the behaviour of users and make analysis based on user activity,and recognize any attacker or malicious behaviour and securing the data of such malicious users. We have demonstrate how the attackers try to perfrom various attacks on users or server like Distributed Denial of service (DDos), and brute-force attack. And admin recognizes these attacks and have the authority to block such attackers. As a result, the suggested approach helps in reaching this level of security and helps in ensuring that data presented in court is credible.

REFERENCES

[1] Air Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms Amanda Davenport ; Sachin Shetty2019 IEEE International Conference on Blockchain (Blockchain)Year: 2019 | Conference Paper | Publisher: IEEE

[2] Haque M M, Hossain S A 2018 National digital forensics framework for Bangladesh (Bangladesh: 3rd Int. Conf. Electr. Inf. Commun. Technol.)

[3] EzhilKalaimannan(2015), Smart Device Forensics - Acquisition, Analysis and Interpretation of Digital Evidences. International Conference on Computational Science and Computational Intelligence (CSCI) Year: 2015 | Conference Paper | Publisher: IEEE

[4] S. Johannes, and C. Michael, "Anti-forensic resilient memory acquisition," Digital Investigation, 2013.

[5] Singh, S., & Singh, N. (2016, December). Blockchain: Future of financial and cyber security. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 463-467). IEEE.

[6] SarunasGrigaliunas, JevgenijusToldinas, AlgimantasVenckauskas, NerijusMorkevicius and RobertasDamasevicius"Digital Evidence Object Model for Situation Awareness and Decision Making in Digital Forensics Investigation" 2020.

[7] Baig, Zubair&Szewczyk, Patryk&Valli, Craig &Rabadia, Priya&Hannay, Peter &Chernyshev, Maxim &Johnstone, Mike &Kerai, Paresh& Ibrahim, Ahmed &Sansurooah, Krishnun& Syed, Naeem& Peacock, Matthew. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation. 22. 10.1016/j.diin.2017.06.015.

[8] F. Marco, B. Alessandro, P. Alessandro, and B. Mauro, "Countering anti-forensics by means of data fusion," 2014.